REMARKS

With this response, no claims are amended, cancelled, or added. Therefore, claims 1-15 and 17-30 are pending.

Status of the Claims

Claims 1-15 and 17-30 are pending in the above-referenced application, and were rejected in the Final Office Action mailed December 30, 2003. Claims 1-15 and 28-30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,341,425 issued to Wasilewski et al. (*Wasilewski*) in view of U.S. Patent No. 4,004,089 issued to Richard et al. (*Richard*). Claims 17-27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,345,101 B1 issued to Shukla (*Shukla*) in view of *Richard*. Applicants respectfully traverse these rejections for at least the reasons set forth below.

Claim Rejections - 35 U.S.C. § 103

Claims 1-15

Applicants respectfully submit that the rejection of these claims under *Wasilewski* and *Richard* is improper because no combination of the references discloses or suggests every element of the claimed invention, as required by MPEP § 2143 to establish a prima facie case of obviousness.

Claim 1 recites the following:

> at least one data bit generator to generate a first, second and third plurality of data bits; and
>
> a combiner function, coupled to the at least one data bit generator, including a network of shuffle units, to combine the third plurality of data bits, **using the first and second plurality of data bits as first input data bits and control signals respectively** of the network of shuffle units.

Applicants note that the claim recites a first plurality of data bits used as **input** data bits, and a second plurality of data bits used as **control signals** of the network of shuffle units.

The Office Action at pages 2 and 3 cites the combiner 156 of *Wasilewski* as disclosing the limitations noted above. Specifically, the Office Action at page 2 asserts: "[*Wasilewski*] shows in Fig. 5 that signals from encryptor is being input in combiner where it controls the process." As Applicants are able to understand this reasoning, the Office Action is asserting that *Wasilewski*'s input signals are the same as control signals for its combiner, and that an input signals control the process of the logic block (combiner 156) to which they are input. Applicants must respectfully disagree.

Applicants first point out that *Wasilewski* is silent regarding the control and/or the functioning of its combiner 156, and merely states: "Combiner/transmitter 156 may combine the encrypted sets of data in any manner suitable for a given application. For example, combiner 156 may perform frequency-division multiplexing. Alternatively, combiner 156 may combine the encrypted data sets using a time-division multiplexing scheme." See col. 12, lines 53 to 66. Thus, *Wasilewski*'s data sets are data that is already encrypted, and is being placed in a combiner that will interleave segments of the different data sets into a single transmission stream in accordance with FDM or TDM. Applicants are unable to understand how *Wasilewski*'s discussion of preparing an encrypted data stream for transmission according to a transmission scheme is purported to disclose or suggest control signals to logic blocks. There is no discussion in *Wasilewski* about how the input data sets, as apparently asserted by the Office Action, are purported to control how the different data sets are to be prepared for transmission. Thus, Applicants must respectfully submit that *Wasilewski* provides no direct support for the assertion in the Office Action.

Furthermore, Applicants next point out that the assertion in the Office Action fails as a matter of logic. An input to a logic function does not "control the process." For example, if inputs 0 and 1 were inputs to an AND gate, the process would be the ANDing of the inputs, and the result (the outcome) would be 0. Changing the inputs to 1 and 1 would not alter the process, which would continue to be the ANDing of the inputs, even though the outcome would change to 1. Applicants submit that this would hold true for a non-logic function, such as the combining of data sets for transmission according to TDM or FDM, as cited in the Office Action.

Applicants respectfully point out that MPEP § 2111 states that "during patent examination, the pending claims must be given their broadest **reasonable** interpretation **consistent with the specification**," and that "the broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach." Applicants again note that the claim recites both "input data bits" and "control signals" in the claims. Were these two terms interpreted to be analogous, the interpretation would render one of the terms redundant, and would fail to give meaning to the words of the claims. Thus, Applicants respectfully submit that the reasoning used to support the rejection of claim 1 fails as a matter of logic, and fails to find support in the cited references.

Furthermore, *Richard* is cited only as disclosing a shuffle unit, and fails to cure the deficiencies of *Wasilewski* set forth above. Therefore, Applicants respectfully submit that either alone or in combination, the cited references fail to disclose or suggest every element of claim 1.

Claims 2-15 depend from claim 1. Because dependent claims necessarily include the limitations of the claims from which they depend, Applicants respectfully submit that these claims are not rendered obvious by the references for at least the reasons set forth above.

Claims 28-30

Claim 28 recites the following:

> generating a first, second and third plurality of data bits; and
> shuffling and propagating a fourth data bit generated from the first plurality of data bits, **under the control of the second plurality of data bits**, to output a fifth data bit to combine the third plurality of data bits.

Applicants note that the limitations of these claims were not directly addressed in the Office Action, but were merely rejected under the same rejection of claims 1-15, discussed above. To the extent that the Office Action is attempting to extend to the limitations of this claim the above-referenced assertion that input data bits are control bits, Applicants refer to the above discussion of how the assertion in the Office Action fails for both reasons of logic and lack of support in the cited references. Furthermore, to the extent that either *Wasilewski* or *Richard* discuss controlling shuffling, Applicants note that *Richard* at col. 6, lines 49 to 51 states: "The position of 56 jumper wires in the mating plug determines the bit interchange," thus implying that the process is controlled by hard-wiring the hardware. Thus, Applicants respectfully submit that the cited references, either alone or in combination, fail to disclose or suggest at least shuffling under the control of a second plurality of data bits, as recited in the claim. Therefore, Applicants submit that claim 28, and its dependent claims 29-30, are not rendered obvious by the cited references.

Claims 17-27

Applicants respectfully submit that the rejection of these claims under *Shukla* and *Richard* is improper because no combination of the references discloses or suggests every element of the claimed invention, as required by MPEP § 2143 to establish a prima facie case of obviousness.

Claim 17 recites the following:

> a first XOR gate to receive a first plurality of data bits and combine them into a second data bit;
>
> a network of shuffle units, coupled to the first XOR gate, to output a third data bit by shuffling and propagating the second data bit through the network of shuffle units **under the control of a fourth plurality of data bits**; and
>
> a second XOR gate coupled to the network of shuffle units to combine a fifth plurality of data bits using the third data bit;
>
> wherein at least one of the shuffle units comprises a first and a second flip-flop to store a first and a second state value, and **a plurality of selectors coupled to the first and second flip-flops to control selective output of one of the first and second state values based on a corresponding one of said fourth plurality of data bits.**

Applicants respectfully point out that the Office Action fails to discuss the limitations of the claim highlighted above. The bare assertion in the Office Action on page 5 that "*Shukla* explicitly shows the limitations, recited in the independent claim 17, in Fig. 3" fails to point out what in *Shukla* is purported to show, explicitly or otherwise, the limitations recited in claim 17. Applicants note that Fig. 3 of *Shukla* merely shows a block diagram with blocks consisting of: a plaintext starting point, and encryption rounds having an XOR1 operation, a shuffle operation, and an XOR 2 operation. Fig. 3 fails to explicitly show either the control of the XOR operations, or a plurality of selectors as recited in the claims. Nor has the Office Action pointed to anything in Fig. 3 or any of the text of *Shukla* that is purported to disclose or suggest these elements of the claimed invention. Nor has the Office Action provided any reasoning to suggest how *Shukla* may be interpreted as disclosing these items. Furthermore, the Office Action cites *Richard* only as disclosing a shuffle unit, and fails to point to anything in *Richard* that is purported to disclose or suggest the limitations discussed above. Therefore, Applicants must submit that the Office Action has failed to provide a complete rejection of claim 17, and are unable to respond to the rejection of this claim until such time as a prima facie case of anticipation or obviousness is provided.

Claims 18-27 depend from claim 17, and thus necessarily include the limitations of the independent claim from which they depend. Therefore, Applicants submit that a complete rejection for these claims is likewise missing in the Office Action. Therefore, Applicants are unable to respond to the rejection of these claims.

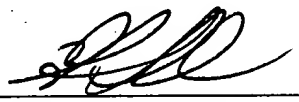
Conclusion

For at least the foregoing reasons, Applicants submit that all rejections have been overcome. Therefore, Applicants submit that all pending claims are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application.

Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: 2/27/04



Gregory D. Caldwell
Reg. No. 39,926

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
Telephone: (503) 684-6200

GDC/VHA